

### **REMARKS**

[0002] Claims 1, 3-7, and 9-30 are pending in the present application. Claims 1, 3, 9-14, 17-24, and 27-29 stand rejected under §102(e) as being anticipated by Grawrock. Claims 4-8, 15, 16, 25, 26, and 30 are rejected under §103(a) as being unpatentable over Grawrock and Zimmer et al. (US Pub. 2005/0021968) (hereinafter “Zimmer”). Applicants have amended Claims 1, 4, 9, 19, 29, and 30.

### **AMENDMENTS TO CLAIMS**

[0003] Applicants have amended Claims 1, 4, 9, and 19 to clarify that the cryptographic key is combined with the measurement values for one or more of a BIOS, a boot record, a drive serial number, and an object code image of decryption code software in at least one PCR. Support for this amendment is found in paragraph 21 of the specification, which notes that: “[i]n one embodiment, the cryptographic key is sealed to a ‘digital fingerprint’ that represents the embedded firmware including a BIOS, a boot record, a drive serial number, and an object code image of decryption software.”

[0004] Claim 29 specifies means for sealing a cryptographic key associated with a data repository to the measurement value for two or more of a BIOS, a boot record, a drive serial number, and an object code image of decryption code software, the measurement value representing the device, to produce a sealed key. Support for this amendment is similarly found at least at paragraph 22.

[0005] Claim 30 specifies sealing the cryptographic key using the drive serial number associated with the data repository. Support for this amendment is found at least in paragraphs 22 and 48.

### RESPONSE TO CLAIM REJECTIONS UNDER §102(e)

[0006] It is well settled that under 35 U.S.C. §102 “an invention is anticipated if... all the claim limitations [are] shown in a single art prior art reference. Every element of the claimed invention **must be literally present**, arranged as in the claim. The identical invention must be shown in as complete detail as is contained in the patent claim.” *Richardson v. Suzuki Motor Co., Ltd.*, 9 USPQ 2d 1913, 1920 (Fed. Cir. 1989) (emphasis added). Appellants respectfully assert that every element of the amended Independent Claims is not present in Grawrock.

[0007] As amended, the independent claims recite that the key associated with the data repository is sealed by cryptographically combining the key with the measurement values for one or more of a BIOS, a boot record, a drive serial number, and an object code image of decryption software in at least one platform configuration register (PCR). The independent Claims further specify that the measurement values represent a trusted configuration of the trusted computing platform.

[0008] By using one or more of these targets for the measurement values, the key is sealed to the particular configuration of the platform. The insertion of snooperware in the BIOS, for example, or a drive swap would be detected and the key would not be unsealed. In this situation, the integrity of the hard drive that is encrypted with the sealed key would not be compromised.

[0009] Grawrock discusses using “digest values” stored in the PCRs as part of an encryption scheme (see, e.g., Col. 7, 1-20) and storing “integrity metrics” in the PCRs. Col. 5, 45-61. However, Grawrock does not teach or disclose using measurement values

for one or more of the BIOS, a boot record, a drive serial number, and an object code image of decryption software in one or more PCRs to seal a cryptographic key associated with a data repository by cryptographically combining the key with the measurement values.

[0010] Similarly, as to Claim 29, Grawrock does not disclose or teach using two or more of the BIOS, a boot record, a drive serial number, and an object code image of decryption software in one or more PCRs. Nor does Grawrock teach the more specific limitation of using the drive serial number as claimed in Claim 30.

[0011] Because Grawrock does not teach the above limitations, Applicants respectfully submit that Grawrock does not anticipate the amended Claims under §102(e), and as such the Claims are in condition for allowance.

#### RESPONSE TO CLAIM REJECTIONS UNDER §103(a)

[0012] Independent Claims 4 and 30 stand rejected under §103(a) as being unpatentable over Grawrock in view of Zimmer. As discussed above, Grawrock does not teach the amended limitations added to the independent Claims, including Claims 4 and 30. Applicants respectfully assert that Zimmer similarly fails to teach the amended limitations. As such, it would not have been obvious to one of ordinary skill in the art to combine the two references and arrive at the present Claims, which include a limitation taught by neither of the references.

### CONCLUSION

[0013] As a result of the presented amendments and remarks, Applicants respectfully assert that pending Claims 1, 3-7 and 9-30 are patentable and in condition for prompt allowance. Should the Examiner require additional information, Applicants respectfully request that the Examiner notify them of any such need. If any impediments to the prompt allowance of the claims can be resolved by a telephone conversation, the Examiner is respectfully requested to contact the undersigned.

Respectfully submitted,

Date: February 28, 2008\_\_

Kunzler & McKenzie  
8 E. Broadway, Suite 600  
Salt Lake City, Utah 84101  
Telephone: 801/994-4646

\_/David J. McKenzie/ \_\_\_\_\_

David J. McKenzie  
Reg. No. 46,919  
Attorney for Applicants